|  |  |  |  |
| --- | --- | --- | --- |
| **Section** | **Question** | **Type** | **Choice** |
| Authority Bias | You receive a file approval request from the “CEO’s assistant” titled “Q2 Financial Audit – Internal Only,” marked as urgent. You don’t typically report to the CEO. What do you do? | Single Choice 1-4 | A. Open the file to check its contents B. Reply and ask for the sender’s identity C. Contact a superior to verify the authenticity of the instruction D. Ignore the request |
| Authority Bias | If the sender is labeled as “Chief Information Officer,” but the email has a subtle typo in the domain (e.g., admin-secuer), would you still trust it? | Single Choice 1-4 | A. Yes B. Decide based on the content C. Feel suspicious but might still click D. Clearly refuse |
| Authority Bias | If an email praises your recent work in a meeting and invites you to join an “Executive Strategy Group,” are you more likely to click the link? | Single Choice 1-4 | A. Click the link immediately to confirm the opportunity B. Carefully check the email address and link domain for authenticity C. Contact your direct supervisor or HR to verify the legitimacy D. Ignore the email, suspecting it to be a scam |
| Authority Bias | You’re asked to provide a departmental contract copy by someone claiming to be the company’s legal counsel, allegedly with CEO approval but no evidence. What do you do? | Single Choice 1-4 | A. Send the file directly, trusting the person’s identity B. Ask for the legal consultant’s official company email and request to communicate via formal channels C. Notify your department supervisor and respond only after confirming the person’s identity D. Delete the contact and report the behavior as a social engineering scam |
| Authority Bias | Which of the following “authority roles” would most likely persuade you to comply? | Single Choice 1-4 | A. IT Administrator B. Legal and Compliance Department C. Senior Financial Auditor D. Human Resources Manager |
| Urgency Bias | You receive a text saying your tax info with HR is incorrect and must be fixed within 30 minutes or your salary account will be frozen. You’re away from your computer. What do you do? | Single Choice 1-4 | A. Immediately use your phone to log into the company system and verify the authenticity of the notice B.Click the link in the SMS directly to quickly upload the documents C. Contact HR or the IT department through official channels before taking any action D. Ignore the message and wait to handle it on your computer later |
| Urgency Bias | Does the presence of a countdown or time pressure make it harder for you to assess a message’s legitimacy? | Single Choice 1-4 | A.Yes, time pressure makes me more likely to respond quickly B.No, I ignore countdowns and prioritize verifying authenticity C.It depends — I might trust it if it's a familiar platform D. Not sure |
| Urgency Bias | An email claims your device is infected and asks you to click a link immediately. Your system seems fine. What do you do? | Single Choice 1-4 | 1. Click the link immediately to run the "repair tool" B. Perform a full antivirus scan but avoid clicking the email link for now C. Check whether the sender's email address uses the official company domain D. Delete the email directly and mark it as spam |
| Urgency Bias | Have you ever made poor decisions online while under stress or time pressure? | Single Choice 1-4 | A. Yes, I realized it was a scam afterward B. No, I usually stay calm and verify first C. Possibly, but I'm not sure if it led to any risk D. I don't remember |
| Urgency Bias | Which type of phrasing most compels you to act immediately? | Single Choice 1-4 | A. “Your account will be locked otherwise” B. “Information security anomaly warning” C. “Today only — complete immediately” D. “Company-level security upgrade requirement” |
| Commitment Bias | You filled out a professional-looking survey and submitted your email. Now it asks for your phone number to “complete activation.” What do you do? | Single Choice 1-4 | A) Enter my phone number to join the prize draw, since I already submitted my email anyway B) Check whether the survey URL is official (e.g., ending in .gov, .com, or .org) C) Refuse to provide it, realizing it might be a scam collecting personal information D) Try submitting a fake number first to see if it goes through |
| Commitment Bias | Do you feel compelled to “see things through” even when doubts arise about legitimacy? | Single Choice 1-4 | A. Yes, I tend to persist to the end to avoid “wasting” the information I've already provided B. No, I stop immediately once I become suspicious C. I hesitate, but might eventually give in D. It depends, such as how much I trust the platform |
| Commitment Bias | An old client recommends you try a certification tool. After the first few steps, it asks for your ID copy and signature. Do you proceed? | Single Choice 1-4 | A. Submit it directly because it was recommended by a long-time client B. Pause and contact the client to verify if the request is real C. Ask the requester to provide official credentials before deciding D. Submit only a redacted copy with a watermark stating “For XX use only” |
| Commitment Bias | Which of the following scenarios would most likely make you continue because of prior commitment? | Single Choice 1-4 | A. Already entered a large amount of personal information B. Spent a lot of time browsing the content C. Was recommended by someone earlier D. The system has already promised a reward |
| Commitment Bias | Have you ever thought “I’m already halfway through, might as well finish” while entering personal information? | Single Choice 1-4 | A. Yes, I sometimes do this (continue submitting even when I have doubts) B. No, I stop immediately once I become suspicious (regardless of how much I've already filled in) C. It depends (e.g., on the website’s credibility or the importance of the information) D. Not sure (I haven't really paid attention to my mindset in such situations) |
| Familiarity Bias | A group chat member (not a direct contact) sends you a file saying “Thought you’d be interested in this report.” What do you do? | Single Choice 1-4 | A. Open the file directly out of curiosity about its content B. Privately message the sender to ask about their identity and the purpose of the file C. Scan the file with antivirus software and open it only after confirming it’s safe D. Ignore or delete the file without opening it if it’s from an unknown source |
| Familiarity Bias | A short link (e.g., bit.ly) appears in your official company announcement channel. What do you do? | Single Choice 1-4 | A. Click directly because it was sent through an official company channel B. First check the authenticity of the shortened link (e.g., by hovering to view the actual URL) C. Contact the IT department to confirm whether the link is legitimate D. Refuse to click and request the full URL instead |
| Familiarity Bias | Which of the following makes you least suspicious of a message? | Single Choice 1-4 | A. Appeared in a familiar app (e.g., Slack, WeChat) B. Used internal terms and abbreviations C. Signed by a colleague I frequently communicate with D. Similar content has appeared before |
| Familiarity Bias | Do you feel less guarded when interacting with people you’ve known before, even loose | Single Choice 1-4 | A. Yes, I feel more at ease with links/files sent by people I know B. No, I always verify authenticity regardless of how familiar the sender is C. It depends — I tend to be less cautious with colleagues or classmates D. I haven't really noticed this tendency in myself |
| Familiarity Bias | You see a friend sharing a benefit-registration link on social media. The site looks familiar, but it asks for bank details. What do you do? | Single Choice 1-4 | A. Fill it out directly, assuming it’s safe because a friend recommended it B. Close the page and message the friend privately to check if their account was hacked C. Check whether the website domain matches the official one (e.g., look for spelling errors) D. Report the link and scan my phone with security software |
| **Optimism Bias** | When you receive a "system vulnerability warning", what is your first reaction? | Single Choice 1-4 | A. Immediately check and update the system B. “My device is secure, I don’t need to worry about it” C. Forward it to the IT department for confirmation D. Ignore it and deal with it only if a problem actually occurs |
| **Optimism Bias** | A friend says, “I never install antivirus software and I've never been infected.” How do you respond? | Single Choice 1-4 | A. Agree, thinking security software is unnecessary B. Disagree and share recent ransomware cases as evidence C. Not sure, but I still choose to install protection myself D. Suggest they at least enable the firewall |
| **Optimism Bias** | The company requires all employees to change their passwords. What’s your response? | Single Choice 1-4 | A. “Hackers won’t target me — I’ll just keep using my old password” B. Change it immediately and use a strong, complex password as required C. Change it but use a simple and easy-to-remember combination D. Delay it for a few days before taking action |
| **Optimism Bias** | You see a notice saying “99% of users have installed the security patch.” What do you do? | Single Choice 1-4 | A. “I’m the lucky 1% — no need to update” B. Feel concerned about potential vulnerabilities and update immediately C. Wait until my computer reminds me again D. Manually close the notification |
| **Optimism Bias** | What is your attitude toward news reports about the rise in online scams? | Single Choice 1-4 | A. “That kind of thing would never happen to me” B. Learn about anti-fraud strategies and remind my family to stay alert C. Pay some attention but don’t change my habits D. Think the news is exaggerating the issue |
| Sunk Cost Fallacy | After completing 90% of a prize draw questionnaire, you're asked to enter your bank card number. What do you do? | Single Choice 1-4 | A. “I've already filled in so much — might as well finish it” B. Quit and close the page immediately C. Submit a fake card number D. Contact the organizer to verify the request |
| Sunk Cost Fallacy | An employee has repeatedly leaked data but hasn’t been dismissed due to their business expertise. If they violate the rules again, what would you do? | Single Choice 1-4 | A. “The cost of replacing them is too high — give one more chance” B. Suspend them and re-evaluate their access permissions C. Increase monitoring but avoid disciplinary action D. Attribute the issue to system flaws rather than the individual |
| Sunk Cost Fallacy | You’ve already shared your home address with a stranger online, and they now ask for a photo of your ID card. What do you do? | Single Choice 1-4 | A. “I’ve already given them my address — might as well send the ID too” B. Immediately cut off contact C. Claim you don’t have an ID D. Try to investigate their identity in return |
| Sunk Cost Fallacy | The “free software” you spent two hours downloading is flagged as a virus. What do you do? | Single Choice 1-4 | A. Disable the antivirus and force the installation B. Delete it and run a full system scan C. Test it in a virtual machine D. Assume it’s a false positive and continue using it |
| Sunk Cost Fallacy | A subscription service auto-renews into a high-priced plan. What do you do? | Single Choice 1-4 | A. “I've used it for half a year anyway — might as well keep it” B. Cancel the subscription immediately C. Compare with other services before deciding D. File a complaint about misleading charges |
| Instant Gratification&**Bandwagon Effect** | To speed up handling of client data, your team proposes disabling encryption temporarily. What is your response? | Single Choice 1-4 | A. “Disable it for now — we’ll re-encrypt everything afterward” B. Refuse, and insist on optimizing the encryption algorithm instead of removing it C. Allow it only for non-sensitive data D. Approve the request but limit the disabled period to 1 hour |
| Instant Gratification&**Bandwagon Effect** | To meet a tight deadline, the development team proposes skipping the code security audit. What do you do? | Single Choice 1-4 | A. “Go live first — we’ll fix any vulnerabilities later” B. Delay the launch until the audit is completed C. Audit only the high-risk modules D. Require the developers to personally guarantee the code’s security |
| Instant Gratification&**Bandwagon Effect** | In a tech chat group, several people share a download link for a “new hacker tool” and comment “tested and working!” What do you do? | Single Choice 1-4 | A. “So many people recommend it — it should be safe” → download and run it directly B. Check if the file’s hash value has been publicly verified C. Test it in a virtual machine before making a decision D. Report the link and alert the group admin |
| Instant Gratification&**Bandwagon Effect** | Your company requires complex passwords, but your colleagues are all using simple ones and writing them on sticky notes. What do you do? | Single Choice 1-4 | A. “Everyone’s doing it — I’ll just set an easy one too” B. Stick to using a password manager to generate strong passwords C. Write it down but keep it locked in a drawer D. Complain to the IT department that the policy is unreasonable |
| Instant Gratification&**Bandwagon Effect** | A high-risk vulnerability has been exposed, but your department hasn’t patched it, saying “nothing has happened so far.” What do you do? | Single Choice 1-4 | A. “It might not be that serious — wait and see” B. Apply the patch immediately and flag it as a critical task C. Patch only your own computer D. Send a mass email blaming colleagues for being irresponsible |